37
Elektronische identiteiten en vertrouwensdiensten

Aan de orde is de behandeling van:
- **het wetsvoorstel Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten) (34413).**

De **voorzitter**:
De minister van Economische Zaken was al aanwezig, maar ik heet hem nogmaals van harte welkom. Wij hebben vier sprekers. Wij beginnen met de heer Remco Bosma van de fractie van de VVD.

De algemene beraadslaging wordt geopend.

De heer **Remco Bosma** (VVD):
Voorzitter. Als je net online kleding hebt gekocht en je op de volgende website je persoonsgegevens al vermeld ziet staan, dan is dat schrikken. Je wilt niet dat een ander aan de haal gaat met deze strikt persoonlijke gegevens. We willen profiteren van het gemak van e-commerce, maar 's nachts niet wakker liggen van de vraag of een ander hier misbruik van maakt. Daarvoor werd al in 1995 gewaarschuwd via de film The Net. In die film werd al gewaarschuwd voor identiteitsfraude voordat e-commerce was uitgevonden. Het risico bestond dat je ongemerkt een soort digitale katvanger zou worden. Gelukkig komt niet elke voorspelling uit.

Soms ontstaat een soort wake-upcall en worden passende maatregelen getroffen. Zo werd in 1997 DigiNotar opgericht, een vertrouwensdienst voor de virtuele wereld. Mooi, hoor ik u denken, dan kunnen wij nu veilig gaan slapen. De ontwikkelingen in de virtuele wereld zijn echter doorgegaan. Er is een breed scala aan mogelijkheden bij gekomen. Sociale netwerken verschenen maar ook de mogelijkheid om gemakkelijk overzeese handel te drijven en online betalingen te doen. Internationale bankzaken regelen we nu massaal in een paar kliks.

Met de toegenomen mogelijkheden om transacties op het internet te verrichten is ook de interesse van criminelen gewekt. Dat betekent dat het zeer belangrijk is dat je weet met wie je te doen hebt en dat je met de juiste persoon te maken hebt. Niet alleen het internet is mondiaal, cybercrime ook. De competitie vindt plaats met de beste criminelen. Wij hebben te maken met een internationaal speelveld en mondiale tegenstanders. Continue waakzaamheid is derhalve geboden. Daar ging het helaas mis, want DigiNotar uit Beverwijk werd in 2011 gehackt. DigiNotar verloor per direct het vertrouwen en ging failliet.

Op dit moment zijn er verschillende nationale richtlijnen en eisen binnen de EU waaraan lidstaten moeten voldoen. Dit zorgt voor een kakofonie en helpt niet om te komen tot een eengeworden digitale Europese markt, want wij weten niet of het allemaal even betrouwbaar is. De Europese verordening biedt uitkomst en stelt kwaliteitseisen aan de vertrouwensdiensten. Wij passen de Telecomwet daar vandaag aan aan. De VVD is daar positief over. Beveiliging is echter zo sterk als de zwakste schakel. Continue waakzaamheid is vereist, want je bent zo outdated. Vandaar dat ik graag van de minister wil weten hoe er goed bij de les gebleven wordt, want de laatste stand der techniek moet de norm zijn en blijven.

Is de taakafbakening tussen BZK en EZ als het gaat om het toelaten van authenticatiemiddelen al opgelost? BZK heeft het voortouw wat betreft eID, maar er zit weinig schot in deze zaak. Hoe hangt dit samen met de eidas-verordening? Wordt het doel van deze verordening wel bereikt als BZK achterloopt met het eID-proces? De taakverdeling gaat over van de ACM naar het Agentschap Telecom. Krijgt het Agentschap Telecom afdoende mogelijkheden om de voor deze taak benodigde specifieke kennis en middelen te verwerven? En zijn de audits die gehouden gaan worden afdoende diepgaand?

Over de waarborgen en de Europese erkenning van vertrouwensdiensten uit derde landen rest nog een laatste vraag. Het is nu niet duidelijk of het toezicht in die derde landen op de vertrouwensdiensten ook wordt meegenomen, terwijl dat in de verordening wel expliciet staat beschreven voor de lidstaten zelf. De vertrouwensdiensten die via derde landen geboden worden, mogen geen veiligheidsrisico vormen voor onze slechts deels eengemaakte digitale markt. Zou de minister hierop willen ingaan?

Mevrouw **Agnes Mulder** (CDA):
Voorzitter. Het CDA staat achter het doel van dit wetsvoorstel, namelijk het vertrouwen vergroten in elektronische transacties. De doeltreffendheid van publieke en private onlinediensten en -handel in de interne markt van de Europese Unie moet goed geregeld zijn. Mijn fractie heeft nog een paar vragen over het borgen van de veiligheid en de privacy, over de uitvoering en toezichtslasten van het wetsvoorstel, en over de toegankelijkheid voor mensen met een handicap.

Ik begin met de vragen over de veiligheid, de privacy en de uitvoering van het wetsvoorstel. Met het wetsvoorstel wordt een knooppunt geïntroduceerd dat moet gaan dienen voor grensoverschrijdende acceptatie van elektronische identificatiemiddelen, het eidas-knooppunt. Kan de minister aangeven in hoeverre dit systeem kinderziektes heeft gekend? Hebben zich in de afgelopen periode nog technische problemen voorgedaan?

Bij de inrichting van het knooppunt hebben de lidstaten gekozen voor een gedecentraliseerde structuur, waarbij ieder land één of maximaal enkele knooppunten heeft. Kan de minister aangeven waarom de keuze hierop is gevallen? Kan deze inrichting eventueel leiden tot risico's op het gebied van de veiligheid? En zo ja, welke zijn dat dan? Zijn die risico's lager dan wanneer men had gekozen voor een gecentraliseerde structuur?

Klopt het dat het knooppunt uitsluitend de voornaam, de achternaam, de geboorteplaats en de geboortedatum uitwisselt? Zullen deze gegevens altijd worden versleuteld?

Kan de minister daarnaast wat verder ingaan op de situatie dat bij niet-gekwalificeerde vertrouwensdiensten minder strenge technische beveiligingseisen worden toegepast in verband met het gebruiksgemak en de kosten? Volgens de minister hebben de gebruikers aangegeven het acceptabel te vinden als de waarborgen minder groot zijn voor sommige doeleinden. Dat stond op pagina 10 van de nota naar aanleiding van het verslag. Kan de minister aangeven over welke doeleinden gesproken wordt? Bij welk onderzoek hebben gebruikers dit aangegeven?

Het CDA heeft ook vragen over het opslaan van gegevens.

Mevrouw **Oosenbrug** (PvdA):
Ik vind dit heel interessant, want dit gaat om de versleuteling van gegevens. Ik weet dat het CDA een groot pleitbezorger is van het stoppen met encryptie. Het CDA geeft hier duidelijk aan waarom het belangrijk is dat deze gegevens versleuteld worden, maar in een ander debat gaf het CDA juist aan van die versleuteling af te willen. Hoe verhoudt dat zich met elkaar? Ik hoor graag waarom versleuteling in dit geval wel belangrijk is, terwijl het CDA er in andere discussies vanaf wil.

Mevrouw **Agnes Mulder** (CDA):
Dit gaat over je voornaam, je achternaam, je geboorteplaats en je geboortedatum. Stel dat ik als inwoner van Nederland bij een buitenlandse overheid terechtkom. Hoe werkt het dan met mijn gegevens? Als je als inwoner van Nederland in Griekenland naar de politie moet omdat je portemonnee gejat is of wat dan ook, wordt er dan op een goede manier met je gegevens omgegaan? Die vraag leg ik hier voor aan de minister. Er zijn daarnaast nog een aantal andere typen diensten. Hoe wordt daartegen aangekeken? Hoe zit het dan met de toezichtslasten en de administratieve rompslomp? Die vragen stellen wij aan de minister en ik ben heel benieuwd hoe hij dat ziet. Maar misschien kan mevrouw Oosenbrug verduidelijken over welke situaties zij het heeft. Ik kan daar ook in de tweede termijn op terugkomen. Het zal vast te maken hebben met wat mijn collega Van Toorenburg heeft gezegd over veiligheid, maar dat heeft misschien wel een andere achtergrond.

Mevrouw **Oosenbrug** (PvdA):
Dat klopt; vandaar de verhelderende vraag. Je ziet heel duidelijk waarom encryptie belangrijk is. Ik denk dat de minister straks ook gaat uitleggen waarom het belangrijk is dat deze gegevens versleuteld verstuurd worden. Als je in debatten over andere wetgeving zegt dat je alle versleuteling wilt weghalen, heeft dat direct gevolgen voor deze wetgeving. Maar ik wil er best later verder over discussiëren.

Mevrouw **Agnes Mulder** (CDA):
Het lijkt mij heel goed als de minister daar straks op ingaat. Dan kunnen we in tweede termijn altijd nog bekijken waar ruimte zit om elkaar te vinden.

Het CDA heeft ook vragen over het opslaan van de gegevens. De minister geeft aan dat het eidas-knooppunt geen identiteitsgegevens mag opslaan. Hij stelt echter ook dat identiteitsgegevens wel kortstondig mogen worden opgeslagen om, bij een incident, de uitwisseling van berichten in de juiste volgorde te kunnen reconstrueren, zodat plaats en aard van het incident kunnen worden vastgesteld. Maar hoe lang is "kortstondig"?

Het CDA is ook benieuwd hoe storingen voorkomen kunnen worden. De minister heeft op vragen van de Kamer aangegeven dat inwoners en bedrijven niet de dupe mogen worden van een mogelijke storing. Hoe gaat de minister daarvoor zorgen?

He College bescherming persoonsgegevens heeft gepleit voor een aanvullend privacy impact assessment, zodat er een zorgvuldige uitwerking van het knooppunt komt. Hoe staat het met dat aanvullende privacy impact assessment? Gaat de minister dat ook doen?

Dan kom ik bij de toegankelijkheid voor personen met een handicap. De verordening bevat geen criteria voor de toegankelijkheid voor personen met een handicap. Die zijn volgens de minister niet nodig, omdat er in Nederland geen praktijksituaties bekend zijn waarbij personen met een handicap die een vertrouwensdienst wilden gebruiken, dat vanwege hun beperking niet konden doen. Als dat zo is, vraagt het CDA zich af waarom het kabinet dan wel verwacht dat de verplichting van Webrichtlijnen kan leiden tot een disproportionele toename van de kosten en de administratieve lasten. Als vertrouwensdiensten al geheel toegankelijk zijn, zou een verplichting van Webrichtlijnen toch niet leiden tot een disproportionele toename van de administratieve lasten? We krijgen graag een toelichting van de minister hierop. Kan de minister aangeven hoe hij ervoor gaat zorgen dat de wijziging geen negatieve effecten heeft op de toegankelijkheid van de telecomdienst en/of de identiteitscheck, mede in het licht van het VN-verdrag?

De minister geeft verder aan dat onder het Nederlandse voorzitterschap is onderhandeld over een richtlijn van de Europese Unie die de toegankelijkheid van websites, met name overheidswebsites, verplicht stelt. De vraag is in hoeverre deze standaard niet alleen voor overheden maar ook voor bepaalde bedrijven zou moeten gaan gelden. Kan de minister aangeven hoever de onderhandelingen gevorderd zijn? En aan welke bedrijven wordt dan gedacht? We vernemen graag het standpunt van de Nederlandse regering.

Dan kom ik bij het toezicht. Kan de minister nader toelichten waarom het wetsvoorstel een overgang van het toezicht van de Autoriteit Consument & Markt naar het Agentschap Telecom regelt? Verwacht de minister hierbij ook overgangsproblemen?

Ik sluit af met een wat technischere vraag. In de beantwoording lezen we dat voor het toezicht op de verordening 7 extra fte wordt ingezet. Kan de minister nader toelichten waaruit de kosten — ruim 1 miljoen euro — bestaan? In hoeverre kunnen de kosten nog verder omlaag? Wegen de kosten wel op tegen de baten?

☐

Mevrouw **Oosenbrug** (PvdA):
Voorzitter. Nederland heeft een open economie met een uitstekende ICT-infrastructuur. Wij willen onze transacties elektronisch door heel Europa kunnen afhandelen. De Europese Commissie stimuleert de ontwikkeling van één

Europese digitale markt, waarin de nationale eID-systemen gebruikt kunnen worden voor grensoverschrijdende, veilige transacties.

Deze verordening biedt nieuwe kansen voor bedrijven en burgers. Daarom is de Partij van de Arbeid voorstander van deze verordening. Wel moet er rekening worden gehouden met een aantal risico's op het gebied van veiligheid en privacy. Bij de ontwikkeling van gebruiksvriendelijke en innovatieve diensten moet men erop kunnen vertrouwen dat die dienst vervolgens ook zorgvuldig en betrouwbaar kan worden geleverd. Dat betekent dat er zekerheid nodig is over de identiteit van een burger, consument en werknemer, maar ook van de overheid, het bedrijf of de organisatie waarmee je zaken wilt doen. Nu de overheid/het bedrijf en de burger/de consument elkaar online en niet altijd meer face to face ontmoeten, is er behoefte aan een vergelijkbaar niveau van zekerheid over de identiteit van degene met wie je zaken doet.

De PvdA heeft in de schriftelijke ronde al veel kritische vragen gesteld. Ik bedank de minister en zijn ambtenaren voor de uitgebreide beantwoording. Toch blijven er nog wel een paar vragen over, die ik graag aan de minister voorleg. Wanneer burgers en bedrijven gebruikmaken van onlinedienstverlening, moet er sprake zijn van een veilige omgeving. Nu ligt de verantwoordelijkheid voor het melden van een lek bij de lidstaten, zo lezen wij in de beantwoording. De PvdA maakt zich zorgen over de eventuele gevolgen van zo'n lek. Het toezicht op de lidstaten kan wat mijn fractie betreft een heel stuk beter. Welke concrete plannen heeft de minister voor ons in petto om deze zorg toch wat weg te nemen?

Ook vragen wij ons af waarom de minister het Nationaal Cyber Security Centrum niet vooraf een meer controlerende functie verleent, in plaats van achteraf correctief. De PvdA hecht veel waarde aan privacy bij onlinedienstverlening. Binnen de wetswijziging bestaat nog enige onduidelijkheid over de verschillende niveaus van diensten die gebruikmaken van onze digitale handtekeningen en andere onlinegegevens. In de beantwoording lezen we dat er gestreefd wordt naar een "voldoende mate van vertrouwelijkheid". De PvdA-fractie vindt deze zinsnede echt te vaag en wil dan ook een helderdere specificatie van de minister.

Ook zijn wij net als de collega van het CDA benieuwd naar de resultaten van het aanvullende privacy-assessment, dat volgens de beantwoording uitgevoerd moet zijn. Ik hoor graag een reactie van de minister hierop.

☐

Mevrouw **Klever** (PVV):
Voorzitter. Het doel van dit wetsvoorstel is veilige elektronische identificatie tussen burgers, bedrijven en overheden in de EU. In de kern moet het de betrouwbaarheid van elektronische identificaties vergroten, zodat deze identificaties Europabreed gebruikt kunnen worden. Je kunt je straks als Nederlander met je DigiD identificeren als je je inschrijft aan een Spaanse universiteit, of als je btw terugvraagt van de overheid van Letland als je daar zaken doet.

Het grootste bezwaar van de PVV tegen dit wetsvoorstel is dat er te gemakkelijk van uit wordt gegaan dat elektronische identificatie veilig is mits je aan een aantal randvoorwaarden voldoet. Die aanname is wat ons betreft onjuist. Zo lazen we afgelopen week in Het FD dat er sprake was van een verdubbeling van schade door zakelijke identiteitsfraude. Dat was pas het topje van de ijsberg, want veel bedrijven melden het niet eens, uit angst voor imagoschade. Ook van banken is bekend dat ze regelmatig het slachtoffer worden van elektronische fraude. Omdat banken veel waarde hechten aan internetbankieren, worden particulieren zeer coulant behandeld als ze schade oplopen als gevolg van identiteitsfraude. Burgers worden inmiddels via de bekende reclameslogan "hang op, klik weg, bel uw bank" actief gewaarschuwd voor digitale fraude in Nederland. Enig wantrouwen over wat er met je digitale gegevens gebeurt, lijkt dus wel op zijn plaats.

Dit wetsvoorstel vergroot de mogelijkheden om digitale persoonsgegevens uit te wisselen. Daarmee vergroot het ook de mogelijkheid dat je persoonsgegevens ergens in het buitenland door criminelen worden opgepikt. Als Oost-Europese bendes zich bijvoorbeeld in Bulgarije toegang verschaffen tot het Bulgaarse elektronische identificatiesysteem, staan daar straks ook persoonsgegevens in van Nederlandse burgers. Dat lijkt ons onwenselijk. De waarborgen en meldingsplicht die in dit wetsvoorstel zijn opgenomen, zullen dit misbruik niet verhinderen, zo verwachten wij. Dat blijkt bijvoorbeeld ook uit het feit dat wij meenden dat wij met DigiD de zaken in Nederland digitaal goed voor elkaar hadden. Toch bleken criminelen beslag te kunnen leggen op DigiD-codes van mensen, om hiermee uitkeringen, toeslagen en studiefinanciering weg te sluizen. Het lijkt ons dus zaak om ieders digitale gegevens juist zo veel mogelijk af te schermen in plaats van deze door heel Europa te verspreiden.

Je kunt bij een bank geen rekening openen zonder je uitgebreid fysiek te identificeren. Een notaris passeert geen onroerend goed als partijen zich niet fysiek hebben gelegitimeerd. Maar wij vrezen dat deze verordening het op Europees niveau straks mogelijk maakt om allerlei belangrijke zaken te regelen zonder dit soort fysieke waarborgen. De PVV onderschrijft dat elektronisch zakendoen steeds belangrijker wordt en dus gefaciliteerd moet worden, maar zo'n ontwikkeling moet wel op een evenwichtige wijze plaatsvinden, waarbij burgers en bedrijven worden beschermd tegen oneigenlijk gebruik. Dat evenwicht missen wij. Het was juist de achteloosheid op het gebied van digitale veiligheid waar toenmalig Ombudsman Brenninkmeijer al voor waarschuwde. De PVV wil onze digitale veiligheid niet te grabbel gooien en zal daarom tegen de uitvoering van deze EU-verordening stemmen.

De heer **Remco Bosma** (VVD):
Volgens mij is deze verordening juist bedoeld om kwaliteitseisen te stellen. Dat betekent dat de huidige praktijk wordt verbeterd. Ik snap daarom de uitspraak van mevrouw Klever dat zij tegen deze verordening of in ieder geval tegen deze wetsaanpassingen wil stemmen, niet. Daar komt nog bij dat het ook geen zin heeft. We passen de wet alleen op een rechtstreeks geldende verordening aan; het heeft dus eigenlijk ook geen zin om ertegen te stemmen.

Mevrouw **Klever** (PVV):
Zoals bekend hebben wij geen boodschap aan EU-verordeningen. Wij gaan hier in Nederland over onze eigen Nederlandse zaken; dat is punt één. Punt twee is dat een andere instantie straks gaat beoordelen of bijvoorbeeld het

Bulgaarse DigiD-systeem, het elektronische identificatiesysteem, voldoet aan een aantal randvoorwaarden. Zo ja, dan mogen de Bulgaren via identificatie zakendoen met de Nederlandse overheid. Andersom mogen Nederlanders dan ook zakendoen in Bulgarije. Het punt is dat je je persoonsgegevens natuurlijk moet beschermen. Door deze verordening wordt de identificatie met andere landen straks automatisch geregeld. Wij denken juist: als je het in Nederland nog niet eens kunt regelen — kijk naar de schandalen met de DigiD — moet je het dan Europees gaan regelen? Laten we er eerst voor zorgen dat we het hier in Nederland kunnen regelen; dat is al moeilijk genoeg.

De **voorzitter**:
Daarmee is een einde gekomen aan de eerste termijn van de Kamer.

De vergadering wordt van 19.57 uur tot 20.26 uur geschorst.

☐

Minister **Kamp**:
Voorzitter. Mevrouw Klever sloeg de spijker op de kop toen zij zei dat er natuurlijk sprake is van een digitale ontwikkeling. We zien allemaal wat er gebeurt, digitaal en op internet. Mevrouw Klever zegt dat die zaken gefaciliteerd moeten worden. Alleen, vervolgens trok zij de conclusie dat zij tegen de uitwerking is van deze richtlijn van de Europese Unie. Er is echter helemaal geen EU-richtlijn aan de orde. Het gaat om een verordening. Het verschil tussen een verordening en een richtlijn is dat een richtlijn door ons in een wet moet worden omgezet, waarna deze rechtskracht krijgt, terwijl een verordening uit zichzelf in een keer rechtskracht heeft. Nu is sprake van een EU-verordening waarin het gaat om elektronische identificatie en vertrouwensdiensten. Voor vertrouwensdiensten is de verordening al in werking getreden in juli dit jaar. Voor de elektronische identificatie moet dit geregeld zijn in de lidstaten in 2018. Het is onontkoombaar dat dit moet gebeuren in alle lidstaten. Wij gaan nu stemmen over aanpassing van onze regels en uitwerking van de verordening op de punten dat dit nog nodig is. Maar dit is dus allemaal al een feit omdat de verordening rechtstreekse werking heeft.

Mevrouw Klever had groot gelijk toen zij zei dat dit iets is wat gefaciliteerd moet worden omdat het een gegeven is. We zijn al sinds de jaren negentig bezig met dit onderwerp. We hadden ook al de richtlijn elektronische handtekeningen, die stamt uit 1999. Deze richtlijn wordt door de verordening vervangen. Deze was er niet voor niks, omdat we ook in Nederland al heel veel doen met vertrouwensdiensten, elektronische handtekeningen en elektronische identificatie. Ik noem een paar voorbeelden. Mensen doen bijna allemaal hun belastingaangifte digitaal. Dan ben je dus met dit onderwerp bezig. Studenten zijn een ander voorbeeld. Zij werken met de Dienst Uitvoering Onderwijs (DUO) via een digitaal portaal. Zij doen dat allemaal en vinden dat heel logisch. Zij werken vrijwel niet op een andere manier met DUO. Mensen zonder werk, die met het UWV te maken hebben, zijn een ander voorbeeld. Zij werken met uwv.nl. Dat is ook zo'n digitale dienstverlening. Het is allemaal al gaande.

Je merkt dat het niet alleen binnen Nederland gaande is, maar ook al over de grenzen heen. In Nederland zijn daarvan twee voorbeelden. Op de website van de Rijksdienst voor Ondernemend Nederland (RVO) kunnen Belgische boeren met hun Belgische elektronische identificatie al ontheffingen en vergunningen aanvragen voor het vervoer van mest en voor import en export van planten. Dat is al op die manier met de Belgen gaande. Een ander iets wat we met de Belgen al hebben lopen, is dat een Belg in geval van een verkeersboete sinds kort met zijn Belgische elektronische identificatiemiddel kan inloggen op de website van het Nederlandse Centraal Justitieel Incassobureau. Hij kan dan de foto bekijken waaruit blijkt dat hij inderdaad gedaan heeft waarvoor hij de boete gekregen heeft. Dus ook over de grenzen hebben we dit al lopen. Het is ook heel gewenst dat dit gaat lopen.

Als een Pool heeft gewerkt in de tuinbouw en hij digitaal belasting wil terugvragen, dan kan hij dat vanuit Polen doen. Hij hoeft daarvoor niet naar Nederland om daar handelingen te verrichten. Nee, dit kan gewoon vanuit Polen geregeld worden. Maar een Nederlander die bijvoorbeeld een bedrijf wil beginnen in Estland en die zich bij de Kamer van Koophandel in Estland wil inschrijven, kan dat dan ook vanuit Nederland doen. Hij hoeft daarvoor niet apart naar Estland. Als je wilt meedoen met een Europese aanbesteding, kun je dat ook vanuit Nederland doen met de elektronische handtekening van KPN, bijvoorbeeld bij een Frans digitaal inschrijfformulier voor een aanbesteding. Het geldt ook voor een Nederlandse student die in Lissabon wil werken. Hij solliciteert en stuurt als bijlage bij een e-mail zijn diploma. In Nederland kan hij dat elektronisch laten waarmerken. Hij kan dat vervolgens op die manier opsturen en hoeft daar niet voor naar Portugal. Ik kan nog een heleboel van dit soort voorbeelden geven. Iedereen snapt dat eigenlijk, omdat we steeds meer samen doen in Europa. Dat willen wij graag en ook de Nederlandse bedrijven willen dit, omdat 70% tot 80% van hun export naar landen in de Europese Unie gaat. Zij willen dat dit graag soepel, makkelijk en zo verantwoord mogelijk verloopt. Daarom ondersteunt Nederland deze ontwikkeling.

Wij hebben al onze eigen ervaring met vertrouwensdiensten en elektronische identificatie. Wij hebben er belang bij dat dit nu ook Europees geregeld is en daarom hebben wij zeer bijgedragen aan deze ontwikkeling. Zo zijn bijvoorbeeld de ervaringen die wij hebben opgedaan bij de DigiNotar-zaak en het advies dat wij daarover gekregen hebben van de Onderzoeksraad Voor Veiligheid, betrokken bij het opstellen van deze verordening. De lessen die in Nederland en in andere landen zijn geleerd op dit punt, zijn verwerkt in deze verordening. Het is de bedoeling dat wij daar nu allemaal in Europa ons voordeel mee gaan doen.

Straks heb je dus de situatie dat er in alle Europese landen datasystemen zijn en dat er ook een toegangsmogelijkheid is gecreëerd voor burgers uit andere Europese landen. Zij kunnen dan naar een bepaald land toe gaan en daar toegang krijgen tot de diensten waartoe ze graag toegang willen hebben. Wij hadden dit kunnen regelen met één Europees systeem, maar dat hebben wij niet gedaan, omdat wij van mening zijn dat landen daar zelf verantwoordelijk voor zijn. Bovendien is het een groter risico als je één centraal Europees systeem hebt. Als het gedecentraliseerd op een goede manier geregeld is en goed gecontroleerd wordt en als je elkaar daar ook op aanspreekt, dan is dat veiliger dan als je één groot systeem hebt. Bovendien wordt dan ook recht gedaan aan de eigen verantwoordelijkheid van

landen. Op die manier hebben wij het geregeld en in deze verordening is dat verder uitgewerkt.

Ik ga nu naar de diverse punten die de woordvoerders aan de orde hebben gesteld. Ik zal op die manier ook wat meer de details in gaan. De heer Bosma vroeg zich af hoe het zit met de toekomstbestendigheid van wat wij nu aan het doen zijn. De techniek ontwikkelt zich voortdurend en hij vroeg zich af of wij de laatste stand van de techniek steeds erbij betrekken en daar steeds gebruik van maken. De heer Bosma had het in dat verband over elektronische identificatie. De eisen die aan elektronische handtekeningen zijn gesteld, zijn in zekere mate technologieneutraal. Dat betekent dat die eisen met de ontwikkeling van de techniek meebewegen. De eisen zijn zo geformuleerd dat, als er technische ontwikkelingen zijn, van die mogelijkheden gebruikgemaakt moet worden.

Bovendien hebben wij drie lagen in de elektronische identificatie aangebracht. Er is een hoge betrouwbaarheid, een substantiële betrouwbaarheid en een lage betrouwbaarheid. Soms kun je met een lage betrouwbaarheid volstaan. Stel dat de heer Bosma informatie wil hebben over iets wat in Slowakije speelt en hij zich daar aanmeldt om die informatie op te vragen, dan kun je met een lage betrouwbaarheid voor wat betreft de elektronische handtekening volstaan. Er zijn namelijk verder geen grote belangen mee verbonden. Je kunt bijvoorbeeld ook meedoen aan een aanbesteding. Daarvoor wil je een aanbestedingsformulier opvragen en vervolgens met een reactie komen. Dan zou je misschien kunnen volstaan met een substantiële hoogte van de betrouwbaarheid. Maar er zijn ook dingen waarbij het heel belangrijk is dat de identiteit heel precies duidelijk is. Dan zijn er hoge eisen aan de betrouwbaarheid. Die verschillende gradaties zijn er dus in aangebracht. Maar de eisen zijn zo veel mogelijk technologieneutraal geformuleerd, zodat wij in die eisen steeds mee kunnen gaan met de ontwikkelingen die zich in de techniek voordoen.

De heer Bosma heeft gezegd dat er weinig schot zit in het eID-traject bij BZK. Hij vraagt zich af op welke wijze dat samenhangt met wat wij hier met eIDAS aan het doen zijn. BZK is daarmee bezig, maar dat is niet een proces dat je zomaar even uit je mouw schudt. We krijgen straks een identificatiestelsel waarin verschillende mogelijkheden zijn ingebracht. Een mogelijkheid is om een chip in te bouwen in de kaart van ons paspoort of rijbewijs, zodat je daar op die manier gebruik van kunt maken. Dat is iets wat technisch ontwikkeld moet worden en vervolgens in een periode van tien jaar ingevoerd zal worden, omdat die documenten die uitgegeven zijn, tien jaar geldig zijn en daarna vervangen worden. De laatste documenten gaan er over tien jaar uit en dan is er een flinke tijd nodig om dat voor iedereen beschikbaar te hebben.

Een tweede mogelijkheid die we hebben, is DigiD. DigiD is een eindige regeling. Er zal nog een verfijning komen, maar op een gegeven moment gaat DigiD eruit. Daar komt iets voor in de plaats als wat wij aan het doen zijn met eHerkenning. Dat wordt verder uitgewerkt en dat wordt dan Idensys. Daar zullen niet alleen bedrijven maar ook burgers gebruik van kunnen maken. BZK is bezig om uit te werken hoe dat hele stelsel er straks uit komt te zien, met verschillende mogelijkheden om op een verantwoorde manier met elektronische identificatie te werken. Dat wordt in een wet afgedekt en vastgelegd. De bedoeling is dat op korte termijn de eerste tranche daarvan in procedure wordt gebracht en dan zijn we daarmee dus verder gekomen.

Wat daar gebeurt, is belangrijk, maar het heeft geen directe invloed op wat wij nu met eIDAS aan het doen zijn. De verordening is voor een deel al in werking, zoals ik al zei, en voor een ander deel moet die in werking gaan treden in 2018. Onafhankelijk van de voortgang van eID en de wetgeving bij BZK zal dit toch gewoon doorgaan.

Zodra wij ons stelsel klaar hebben, waar nu aan gewerkt wordt, kunnen we het aanmelden bij de Europese Commissie. Vervolgens kunnen andere landen ons daarop bevragen. Dan kunnen we erover praten hoe we het opgezet hebben en wat andere landen van de kwaliteit denken. Er is dan een wisselwerking. Vervolgens kunnen we op grond daarvan nog verbeteringen doorvoeren.

Gelijktijdig met het klaar hebben van het stelsel hebben wij ons digitale knooppunt in Nederland dan beschikbaar. Dan kunnen we ook van andere landen gegevens ontvangen. We kunnen ook onze gegevens naar andere landen brengen. Dan begint het proces te lopen. Dat proces van aanmelden, met elkaar erover spreken en het gaan benutten, gaat dus voor alle landen gelden. Op die manier wordt dat stelsel langzamerhand in heel Europa opgebouwd.

De heer **Remco Bosma** (VVD):
Ik heb toch even een vraag over het actueel houden. Aanvankelijk zei de minister dat er eisen zijn geformuleerd die technisch neutraal zijn. Met dat antwoord ben ik heel tevreden, maar over het traject bij BZK zegt de minister: als paspoorten zijn uitgefaseerd, worden zij eventueel voorzien van mogelijkheden om daar iets aan te koppelen. Zo'n paspoort gaat vijf jaar mee. Als er wordt gekozen voor een apart traject via BZK, hoe houden we dan in het snotje dat het veilig blijft, als een paspoort vijf jaar meegaat en de techniek er voor vijf jaar aan vastzit? Ik ben ook bang dat we uiteindelijk een systeem krijgen dat in de commerciële wereld snel navolging krijgt en wordt uitgerold. Vervolgens willen we bij BZK misschien een hoger niveau hebben, maar dan loopt dat achter bij het traject dat in het maatschappelijk verkeer al veel meer gebruikt wordt. Ik zie daar toch nog wel wat risico's in. Kunt u dat specifiek nader duiden?

Minister **Kamp**:
Mijn opmerking over technieknneutraal was geclausuleerd. Er is een bepaalde mate van technieknneutraliteit. Ik denk dat het verstandig is dat we dat gedaan hebben, omdat de ontwikkelingen op die manier verwerkt kunnen worden en er rekening mee gehouden kan worden. Als je een stelsel opbouwt, maak je een publiek middel om iets in te brengen in paspoorten en rijbewijzen waardoor we een hooggekwalificeerd identificatiemiddel hebben. Dan is dat iets wat een bepaalde periode meegaat. Dat gaat zo lang mee als het document geldig is. Als wij het vijf jaar laten gelden, gaat het vijf jaar mee. Als wij het tien jaar laten gelden, gaat het tien jaar mee.

Maar dat is niet de enige mogelijkheid. Private handtekeningen die aan de eisen voldoen, kunnen ook meedoen. Ik heb al aangegeven dat DigiD nog een keer opgewaardeerd kan worden. Ik heb ook aangegeven dat eHerkenning verder uitgewerkt zal worden tot Idensys, en dat het dan ook mee gaat doen. BZK probeert dit stelsel op dit moment op te

zetten. Zodra het stelsel opgezet en wettelijk ingekaderd is met de wet die daarvoor in voorbereiding is, kunnen we het aanmelden. Vervolgens kan het gaan werken vanuit Nederland, zoals het ook vanuit andere landen naar Nederland toe kan gaan werken. Als wij in Nederland de zaak op orde hebben, is het de bedoeling dat het gebruikt kan worden door onze burgers in andere landen van de Europese Unie. Burgers en bedrijven in andere landen van de Europese Unie kunnen ook naar Nederland gaan. Daar hebben we een knooppunt voor in het leven geroepen, dat door mij bij Economische Zaken beheerd zal worden. Op die manier hebben we een gedecentraliseerd stelsel opgezet. Daarbij is ook peer pressure, onderlinge controle, aanwezig, om te zorgen dat de landen waarin zich zwakheden voordoen, die ook oplossen. Op die manier dragen ze bij aan de kwaliteit van het geheel.

De heer Bosma en mevrouw Mulder vroegen hoe het zit met het gegeven dat als toezichthouder in Nederland het Agentschap Telecom wordt ingesteld in plaats van de ACM. Laten we elektronische identificatie en vertrouwensdiensten weer even uit elkaar halen. Over de elektronische identificatie heb ik al gezegd dat de landen elkaar onderling scherp houden. Over de vertrouwensdiensten is in de verordening vastgelegd aan welke eisen ze moeten voldoen, dat er toezicht moet zijn en hoe dat toezicht moet werken. Wij hebben bekeken hoe dat toezicht moet werken en hebben vastgesteld dat de ACM daar niet het beste op toegerust was. Het toezicht is vooral technisch van aard. De meeste deskundigheid over techniek zit bij het Agentschap Telecom. We hebben de know-how bij de ACM overgebracht naar het Agentschap Telecom en gebundeld met de know-how die daar al aanwezig was. Dat hebben we versterkt met extra formatieplaatsen en daar is extra kwaliteit bij ingebracht. Het Agentschap Telecom heeft zich er grondig op voorbereid. Op dit moment is men er klaar voor om de toezichthoudende rol te vervullen. Ik denk dat we dat zo op een goede manier georganiseerd hebben.

De heer Bosma vroeg ook naar de audits die gehouden worden om de vertrouwensdiensten te controleren. Vertrouwensdiensten moeten voldoen aan de eisen die in de verordening zijn vastgesteld. Om te kunnen nagaan of ze daaraan ook voldoen, vindt bij de gekwalificeerde vertrouwensdienstverlener ieder jaar een audit plaats. In Nederland wordt die gedaan door de conformiteitsbeoordelingsinstanties. Dat zijn private bedrijven. Zij maken een extern auditrapport, dat vervolgens naar het Agentschap Telecom gaat. Die zal het bestuderen en bekijken of er nog aanvullende informatie nodig is, dan wel dat de zaak op orde is. Dat gaat jaarlijks gebeuren. Het zijn serieuze audits; er wordt een dag of tien aan gewerkt. In de andere landen moet het op een even serieuze manier gebeuren. De toezichthouder ziet daarop toe. De systematiek daarvoor is in de verordening vastgelegd.

De heer Bosma vroeg ook naar derde landen, landen buiten de Europese Unie. Op dit moment is dat nog niet aan de orde, want er hebben zich nog geen derde landen aangemeld bij de Europese Unie om met hun elektronische identificatie mee te doen, waarmee hun burgers en bedrijven ook elektronisch toegang kunnen krijgen tot diensten in de landen van de Europese Unie. Er is nog geen land geweest dat dit heeft gedaan. Als een land zich ervoor aanmeldt, zal de Europese Commissie beoordelen of de kwaliteit van de organisatie in dat land op dit punt voldoende is. Als dat zo is, kan er met dat land worden gewerkt. Als dat niet zo is, krijgt dat land geen toegang en doet zich daar dan ook geen probleem voor.

Mevrouw Mulder vroeg zich af of er zich bij het eIDAS-knooppunt in Nederland kinderziekten hebben voorgedaan. Dat is niet het geval. Met het eIDAS-knooppunt, dat bij Economische Zaken komt, hebben we al wat ervaring opgedaan. Sinds vorig jaar gebruiken we het al voor pilots met Belgische en Nederlandse grensboeren; ik heb de voorbeelden net genoemd. Ook is de nieuwste programmatuur die we hiervoor gebruiken al actief getest en akkoord bevonden. We hebben er ook al een wisselwerking met de Europese Commissie over gehad, dus wij hebben wat het eIDAS-knooppunt betreft de zaken op orde. Daar doen zich op dit moment geen verdere problemen voor die ik nu met de Kamer heb te bespreken.

Ik ben al ingegaan op de gedecentraliseerde structuur waarvoor gekozen is. We kunnen praten over de vraag of het beter was geweest om het wel gecentraliseerd te doen. Ik denk van niet, maar in ieder geval is die discussie achter de rug, want de verordening is er nu en is voor de vertrouwensdiensten ook al in werking getreden. Ik geloof dus dat dit op een adequate manier is geregeld.

Mevrouw Mulder vroeg mij om te bevestigen dat de gegevens van burgers die in het knooppunt terechtkomen, uitsluitend de voornaam, achternaam, geboorteplaats en geboortedatum betreffen. Ik kan dat bevestigen. Bovendien komen de gegevens er alleen versleuteld in en blijven ze daar maar zeer korte tijd.

Tot mevrouw Klever zeg ik dat die gegevens daar niet twee jaar of een halfjaar blijven staan. Ze blijven er zelfs geen minuten staan. Het gaat om seconden, fracties van seconden die even nodig zijn om in zo'n systeem te checken of het klopt. Als het klopt, wordt er toegang gegeven. De persoonsgegevens zijn dan meteen weer weg uit het knooppunt. Er blijven dus geen persooonsgegevens bewaard in de knooppunten. Het knooppunt heeft ze even vast om te bekijken of het klopt. Als de conclusie wordt getrokken dat dit het geval is, wordt er toegang gegeven en zijn de gegevens meteen weer weg.

Mevrouw **Oosenbrug** (PvdA):
Ik had een aanvullende vraag gesteld. Die data worden opgeslagen, ook al is dat kortstondig. Hoe zorg je ervoor dat ze goed versleuteld worden? Is dat een eis die wordt gesteld? Is er een preventieve bescherming aan de voorkant, zodat de gegevens in ieder geval versleuteld zijn als er op welke manier dan ook een lek is? Hoe belangrijk vindt de minister dat?

Minister **Kamp**:
Ik ben het met mevrouw Oosenbrug eens. Hier zijn drie dingen van belang. Het gaat om beperkte gegevens. Het gaat bovendien om persoonsgegevens die versleuteld zijn. Ten slotte gaat het om gegevens die in de orde van grootte van fracties van seconden bewaard blijven. Dat met elkaar geeft optimale zekerheid.

Mevrouw Mulder sprak over derde landen. Ik ben daar al op ingegaan. Ik heb aangegeven dat zich nog geen derde

landen hebben gemeld. Ik ben ingegaan op de overgang van de ACM naar Agentschap Telecom.

Mevrouw Mulder vroeg ook hoe het zit met de kosten en de baten en hoe die zich verhouden. De verordening vereist dat wij toezicht gaan uitvoeren. Agentschap Telecom heeft daartoe inspecteurs beschikbaar. De kosten bestaan uit de personele kosten van het agentschap; de inspecteurs die het toezicht uitvoeren en de inspecteurs die de audits uitvoeren. De baten bestaan daaruit dat wij daar een zeker stelsel voor terugkrijgen. Wij krijgen zekerheid als gevolg van het toezicht dat wordt uitgeoefend. De kosten die voor dat toezicht worden gemaakt, zijn een fractie van de baten die het uiteindelijk oplevert voor honderdduizenden, zo niet miljoenen burgers en voor honderdduizenden bedrijven die hier gebruik van kunnen gaan maken. Als ergens kosten en baten in goede verhouding staan met elkaar, is dat hier wel het geval.

Mevrouw Mulder vroeg ook naar het tweede impactassessment. Zij zegt dat het College bescherming persoonsgegevens duidelijk heeft gemaakt dat het een tweede impactassessment wil hebben. Dat tweede impactassessment is bijna klaar. Het gaat om de mogelijke aansluiting van het eIDAS-knooppunt op het toekomstige nationale stelsel van elektronische identificatie en authenticatie van burgers en bedrijven. Dat is het stelsel dat op dit moment bij BZK wordt ontwikkeld. Als dat er eenmaal is, moet het eIDAS-knooppunt daarop worden aangesloten. De vraag is dan of dat nu voldoende voor elkaar is wat betreft de privacybescherming. Er is een tweede assessment op losgelaten, ook naar aanleiding van wat er door het College bescherming persoonsgegevens naar voren is gebracht. Dat assessment is bijna klaar. Het is vooral bedoeld voor de situatie dat het stelsel, dat er nu nog niet is, er dan wel is. Dat moet dan worden aangesloten op het knooppunt. Wij praten dus nog over de toekomst, maar toch schat ik in dat wij het assessment nog dit jaar in de maand december bij de Kamer krijgen, zodat u daar ook kennis van kunt nemen. Voor de verordening en voor het wetsvoorstel dat nu aan de orde is, heeft dat geen directe betekenis.

Mevrouw Mulder vroeg ook wanneer de niet-gekwalificeerde vertrouwensdiensten gebruikt kunnen worden. Er zijn twee soorten vertrouwensdiensten. Ze zijn gekwalificeerd of ze zijn niet gekwalificeerd. Mevrouw Mulder vroeg specifiek wanneer de niet-gekwalificeerde vertrouwensdiensten kunnen worden gebruikt en verwees naar bladzijde 10 van de memorie van toelichting. Je moet er dan bijvoorbeeld aan denken dat je een vergunning nodig hebt voor een evenement, of een kapvergunning; in die orde van grootte. Als zich op dat terrein iets afspeelt, is het niet nodig dat je aan de hoogste eisen voldoet en dat het gekwalificeerde vertrouwensdiensten zijn. Dan moet je het ook op een wat eenvoudiger manier kunnen doen. Daarvoor hebben wij die categorie, die daarvoor benut kan worden. Ik denk dat dit een heel praktische manier is om daarmee om te gaan.

Mevrouw Mulder sprak over storingen. Alle lidstaten hebben een eigen eIDAS-knooppunt. Die knooppunten moeten aan de laatste beveiligingseisen voldoen. Als er een storing is, moeten zij dat melden bij de Europese Commissie en aan de andere lidstaten. Dit betekent dat het land vervolgens zelf ervoor moet zorgen dat daar waar er een probleem is, het systeem wordt afgesloten, zodat het probleem meteen geïsoleerd is en zich niet kan verplaatsen. Vervolgens moet men met de andere lidstaten erover spreken wat er moet worden gedaan om dit op te lossen. Dat is de peer pressure waar ik het al eerder over had. Op zo'n manier kan het probleem vervolgens door het desbetreffende land worden opgelost. Elk van de lidstaten heeft groot belang bij het goed functioneren van het hele systeem en bij het goed functioneren van het eigen onderdeel van het totale systeem. Als er een probleem is, moet men dat melden. Vervolgens wordt er gezamenlijk aan een oplossing gewerkt. In het land dat het betreft kan men al meteen de belangrijke eerste stap zetten door af te sluiten wat afgesloten moet worden. Wij zullen dit vanuit Nederland natuurlijk kritisch volgen.

Mevrouw Klever zegt: daar kan mee geknoeid worden. Ja, er kan met alles geknoeid worden. Er kan met bankbiljetten geknoeid worden. Er kan met formulieren geknoeid worden. Je kunt ergens met een paspoort komen waarop een foto van je zus of je broer staat. Alles is denkbaar. Het gaat erom dat wij proberen onze samenleving zo goed mogelijk te organiseren, ook onze digitale samenleving, met het inbouwen van maximale waarborgen. Wij moeten fraude en geknoei zo veel mogelijk tegengaan. Het systeem moet daartegen bestand worden gemaakt. Als zich dan toch problemen voordoen, moeten wij er adequaat op reageren. Het kan niet zo zijn dat we, vanwege het gegeven dat er geknoeid kan worden, zeggen dat we internet maar niet gebruiken of dat we de digitale mogelijkheden maar niet gebruiken. Dat is een onbegaanbare weg. We moeten het wél doen, maar we moeten ook grote aandacht hebben voor de risico's. Alles wat we nu aan het doen zijn, is daar in de eerste plaats op gericht. Wij willen die risico's beperken.

Mevrouw Mulder sprak over de toegankelijkheid van alles voor mensen met een handicap. In al het werk dat we tot dusver hebben gedaan, hebben we niet gemerkt dat zich specifieke problemen voordoen voor mensen met een handicap, anders dan in individuele situaties. Als er in individuele situaties iets aan de orde is, bijvoorbeeld een blinde advocaat die een bepaalde vertrouwensdienst moet gebruiken, dan moet voor haar of hem een persoonlijke oplossing worden gevonden. We zijn beschikbaar om dat te doen. Net als je bankbiljetten en formulieren en paspoorten hebt, heb je ook dit. Je moet dit zo maken dat het door zo veel mogelijk mensen zo goed mogelijk gebruikt kan worden. Daar waar zich individuele problemen voordoen en waar wij daaraan tegemoet kunnen komen, dan moeten wij die bereidheid ook hebben. En die bereidheid hebben wij ook.

Mevrouw Mulder vroeg hoe wij andere dan overheidswebsites toegankelijk laten zijn voor mensen met een handicap. Daar heb ik zo geen antwoord op. Daar gaat dit wetsvoorstel ook niet over. Ik ben ook niet de minister die gaat over andere websites dan overheidswebsites en over de toegankelijkheid daarvan voor mensen met een handicap. Ik stel mevrouw Mulder voor om haar gedachten hierover te wisselen met mijn collega van BZK.

Ik kom op de punten die mevrouw Oosenbrug naar voren heeft gebracht. Als zich ergens bij de elektronische identificatie een lek voordoet, dan moet de desbetreffende lidstaat zelf maatregelen nemen. Die lidstaat moet dat melden en openstaan voor wisselwerking met andere landen om

gezamenlijk tot een oplossing te komen. Vervolgens moet de lidstaat die oplossing ook realiseren. Zo is de verordening opgezet.

Waarom krijgt het Nationaal Cyber Security Centrum niet vooraf een controlerende functie in plaats van achteraf? Het is niet zo dat het centrum een controlerende functie heeft. Het toezicht wordt door Agentschap Telecom verricht. Dat is daar exclusief verantwoordelijk voor. Het Nationaal Cyber Security Centrum van het ministerie van Veiligheid en Justitie is vooral bedoeld om te helpen als er problemen zijn. Dat biedt hulpverlening en geeft advies in geval van incidenten. Agentschap Telecom zorgt ervoor dat iedereen zich aan de regels houdt en dat er in de sfeer van het voorkomen van problemen gedaan wordt wat er volgens de verordening gedaan moet worden. Mochten er vervolgens problemen zijn waar advies of hulpverlening bij nodig is, dan is dat Nationaal Cyber Security Centrum daarvoor beschikbaar. Dat is de opzet die wij gekozen hebben.

Mevrouw **Oosenbrug** (PvdA):
Het Nationaal Cyber Security Centrum heeft ook een andere functie, namelijk dat van een Computer Emergency Rescue Team (CERT), dat in elk land zit. Het zou mij een lief ding waard zijn als dat gewoon wat meer met elkaar gaat samenwerken. Wij hadden het net over Estland. Volgens mij komt er een X-Road voor Europa. Daar kunnen wij op aansluiten. Als daar iets misgaat, is snel ingrijpen wel een vereiste. Dat doe je het beste door vooraf de boel te monitoren. Daarover ging mijn vraag. Waarom zorgen we er niet voor dat het Cyber Security Centrum dat netwerk ook kan monitoren en het vooraf al kan zien als er iets misgaat, in plaats van achteraf te moeten zeggen: er is iets misgegaan en wij gaan jullie helpen? Juist in het vooraf controleren ligt de sleutel tot het vertrouwen hebben in dit systeem. Als je echt het gevoel krijgt dat het van tevoren goed in de gaten wordt gehouden, durf je misschien wat meer je elektronische identiteit te gaan gebruiken. Dat was de strekking van mijn vraag. Ik hoop dat ik die zo wat helderder heb gemaakt.

Minister **Kamp**:
Dit is een Europese verordening. Er zijn regels die nu gelden. Er is ook gezegd dat daar toezicht op moet zijn. Het toezicht moet per land georganiseerd worden en moet aan bepaalde eisen voldoen. Daarin hadden wij zoiets als het Nationaal Cyber Security Centrum ook een rol kunnen geven, maar dat is niet gebeurd. Er is gezegd: er moet in een land een toezichthouder worden aangewezen. Bij ons was dat ACM. Wij hebben de conclusie getrokken dat het het beste is om de toezichthouder Agentschap Telecom te laten zijn. Los van dat toezicht op het systeem en op het handelen dat het agentschap zal uitvoeren, is het nodig om ondersteuning te geven. Voor die ondersteuning is in Nederland het Cyber Security Centrum beschikbaar.

Mevrouw Oosenbrug zei dat het nuttig is om dat ook meer Europees te bezien en te bekijken hoe er tussen de Cyber Security Centra in de verschillende landen kan worden samengewerkt en hoe zij gezamenlijk een goede bijdrage aan het geheel kunnen leveren. Ik denk dat ik op dit punt apart bij de Kamer zal terugkomen, samen met mijn collega van Veiligheid en Justitie. Het is natuurlijk waar dat in al die landen vergelijkbare dingen in de sfeer van hulpverlening en advies worden gedaan. Ik kan me evenals mevrouw Oosenbrug heel goed voorstellen dat dat iets is waarvoor je gezamenlijk dingen zou kunnen doen, wat je gezamenlijk zou kunnen organiseren. Ik ga daar bij een volgende gelegenheid apart op in naar aanleiding van wat mevrouw Oosenbrug naar voren heeft gebracht.

Mevrouw Oosenbrug zei dat er sprake is van het streven naar een voldoende mate van vertrouwelijkheid, maar zij vindt dat vaag. Zij zegt dat zij daarvoor graag een nadere specificatie wil hebben, een nadere toelichting daarop. Voor ondertekening met een elektronische handtekening is vereist dat die voldoende betrouwbaar is voor het doel waarvoor ze wordt gebruikt. Wij zorgen er dus voor dat de veiligheid ten minste even groot is als in de situatie dat er niet elektronisch gewerkt zou worden maar er gewoon, conventioneel verkeer zou plaatsvinden, zoals wij tot dusver hebben gedaan, toen de zaak nog niet gedigitaliseerd was. Het Forum Standaardisatie, het expertisecentrum op dit vlak, heeft een handreiking ontwikkeld om te bepalen welke handtekening in de praktijk voldoende betrouwbaar is voor de verschillende soorten van transacties. Ik heb al aangegeven dat er verschillende varianten mogelijk zijn. De ene keer is het echt noodzakelijk dat de zaak helemaal duidelijk is. Dan moet er een gekwalificeerde elektronische handtekening zijn. Bijvoorbeeld voor het aanvragen van informatie kan het ook mogelijk zijn om met een minder geavanceerde elektronische handtekening te werken. Dat is dan een niet-gekwalificeerde handtekening. Afhankelijk van het gebruik kan een van de twee in aanmerking komen. Ik denk dat dat heel goed is. Het is heel goed om aan bepaalde activiteiten, bepaalde handelingen, standaard de gekwalificeerde elektronische handtekening te koppelen en het voor andere mogelijk te maken om het op een andere manier te doen. Ik geloof dat wij met het gemaakte onderscheid een adequate werkwijze hebben opgezet.

Mevrouw Klever, met wie ik ben begonnen, heeft aangegeven welke problemen zij ziet die zich zouden kunnen voordoen. Aan haar heb ik aangegeven dat zich inderdaad problemen kunnen voordoen. Nu doen zich problemen voor en ook in de toekomst kunnen zich problemen voordoen. Maar het is wel van belang dat we de digitale ontwikkeling faciliteren, zoals mevrouw Mulder ook al zei. Hiermee faciliteren we die ontwikkeling. Hiermee maken we het mogelijk voor Nederlandse burgers om, als zij in andere landen van Europa iets moeten doen, dat op een gemakkelijke manier digitaal te doen. We maken het voor burgers en bedrijven uit andere landen van Europa mogelijk om, als zij in Nederland iets moeten doen, op een gemakkelijke manier toegang te krijgen en hun zaken in Nederland af te werken. Volgens mij is het goed dat we dat doen. Volgens mij hebben we dit nu ook op een verantwoorde manier opgezet. De verantwoorde faciliteit die mevrouw Klever zou willen zien, is dus volgens mij hiermee ingesteld.

Ik zei al dat het een verordening is. Die heeft dus een directe werking. Voor een deel heeft zij die al gekregen per juli van dit jaar. Voor wat betreft de elektronische identificatie moet de verordening haar uitwerking uiterlijk in 2018 krijgen. Wij zijn middels deze wet nu bezig om dat uit te werken, zodat Nederland aan die verordening zal voldoen en Nederlandse burgers daarvan kunnen profiteren. Ik meen dat het in het belang is van die Nederlandse burgers en bedrijven dat er op dit vlak op een verantwoorde manier vooruitgang wordt gerealiseerd. Ik hoop dat ik op deze wijze die overtuiging

ook bij mevrouw Klever heb kunnen creëren. Ik wacht daarvoor de tweede termijn van de Kamer af.

De **voorzitter**:
Dank u wel. Ik vraag de leden of er behoefte is aan het houden van een tweede termijn.

De heer **Remco Bosma** (VVD):
Als ik één vraag mag stellen, voorzitter, heb ik geen tweede termijn meer nodig.

De **voorzitter**:
Gaat u uw gang.

De heer **Remco Bosma** (VVD):
De minister zei dat de audits door commerciële bedrijven worden gedaan en dat daar publiek toezicht op wordt gehouden. Ik wil toch wat lessen trekken uit de Fyra-enquête. Zijn er in het publieke toezicht op de bedrijven die die audits uitvoeren, ook reality checks in de praktijk? Daarbij wordt echt gekeken hoe het in de praktijk gaat en wordt dus niet alleen maar een vinklijstje gevolgd. Kan de minister dus verzekeren dat dit echt diepgaand genoeg is?

Minister **Kamp**:
Ik ken de expertise van de heer Bosma op dit punt. Ik zal mij daarom hier verder in verdiepen naar aanleiding van de aandacht die hij hiervoor vraag. De verantwoordelijkheid ligt bij Agentschap Telecom. Private organisaties doen dit werk. Zij maken die audits en leveren die aan. De heer Bosma zegt: daarbij moet het niet zo zijn dat er alleen maar een lijstje wordt afgevinkt, waarna de zaak wordt goedgekeurd. Hij zegt: er moet ook voldoende diepgang zijn op de momenten dat die nodig is. Dit aandachtspunt van hem heb ik begrepen. Ik zal mij daarin verdiepen op de wijze die de heer Bosma heeft gevraagd.

De heer **Remco Bosma** (VVD):
Ik dank de minister. Als ik het heb over reality checks bedoel ik in dit verband eigenlijk ook te zeggen dat Agentschap Telecom soms net even voorbij de auditorganisatie gaat en in de praktijk bekijkt wat de auditorganisatie op papier heeft staan. Komt die rapportage overeen met wat de mensen van het agentschap zien als ze zelf gaan kijken? Dat is eigenlijk mijn vraag.

Minister **Kamp**:
Ik heb dat goed begrepen. De opmerking van de heer Bosma lijkt mij een reële opmerking die voortkomt uit de praktijk. Hij schetst de manier waarop het agentschap op dit punt zou moeten functioneren. Het lijkt mij logisch dat het zo gebeurt. Ik zal mij hierin verdiepen en zal bekijken hoe dat in de praktijk ingevuld gaat worden.

De heer **Remco Bosma** (VVD):
Dank u wel. Ik ben helemaal tevreden.

De **voorzitter**:
Voor de volledigheid herhaal ik mijn vraag of er bij de andere leden behoefte is aan het houden van een tweede termijn. Ik zie dat dat niet het geval is. Daaruit trek ik de conclusie dat de minister in de eerste termijn de gestelde vragen naar tevredenheid heeft beantwoord. Dat komt niet zo heel vaak voor in de Kamer. Ik dank de minister voor zijn komst naar de Kamer.

De algemene beraadslaging wordt gesloten.